Council of the European Union

PRESS
EN

BACKGROUND[1]
Brussels, 4 June 2018

Transport, Telecommunications and Energy Council (Telecommunications issues) Luxembourg, 8 June 2018

Chair: Ivaylo Moskovski, Bulgarian Minister for Transport, Information Technology and Communications

The **meeting** will **start** at 10.00.

Ministers will hold a policy debate on a proposal to update **privacy rules for electronic communications** (**ePrivacy**). The aim of the debate is to advance the proposal towards a common Council position.

The Council is due to agree a general approach on a proposed **Cybersecurity Act**. The proposal aims to upgrade the current European Union Agency for Network and Information Security (ENISA) into a **permanent EU agency for cybersecurity,** and to create an **EU-wide cybersecurity certification framework for information and communication technology (ICT) products and services.**

Ministers will hold a policy debate on a draft directive to promote the **re-use of public sector information**. The debate will steer future work on this proposal.

The presidency will brief ministers on the latest developments on a **European electronic communications code** and an updated mandate for the **Body of European Regulators for Electronic Communication (BEREC)**. It will also update ministers on the draft regulation on the **free flow of non-personal data**.

The Commission will brief ministers on the state of play of the **digital single market**.

Lastly, the incoming Austrian presidency will present its **work programme**.

Over a working lunch, ministers will discuss digital financial instruments in the context of the multiannual financial framework.

Press conference: +/- 17.00

* * *

Video streaming of press conferences and public events

Video coverage in broadcast quality (MPEG4) and photo gallery

[1] This note has been drawn up under the responsibility of the Press Office.

ePrivacy

The Council will hold a **policy debate** on a proposal to **update privacy rules for electronic communications (ePrivacy**). The draft regulation sets out to ensure a high level of protection of private life, communications and personal data in the electronic communications sector. It also aims to create a level playing field for providers of various services and to ensure free movement of electronic communications data and services in the EU. It will replace the current ePrivacy directive, which was last updated in 2009, and complement the general data protection regulation that became applicable on 25 May.

The document prepared by the presidency for the Council also contains a **progress report** on the technical discussions within the Council.

Under the Commission proposal on e-privacy, confidentiality of communications would apply to both the content of the communication and to metadata - for example who was called, the timing and location of the call and websites visited. The proposal also includes stronger rules on spam and marketing calls.

The scope of privacy rules would be extended to cover not only traditional telcos, but also providers of new services such as VoIP or instant messaging apps and web-based e-mail.

Consent would be required to access information on a user's device. New rules on cookies would shift consent to the browser level in order to give users more control over their devices. No consent would be needed for non-privacy-intrusive cookies that improve the internet experience, such as shopping cart history reminders.

In the Council, the working party has made considerable progress on the proposal. Key issues in the discussions have included the relationship between ePrivacy rules and the general data protection regulation, permitted processing of metadata, and software providers' obligations regarding privacy settings. However, further work is needed before the Council is able to form its position. In order to advance towards this goal, the presidency is asking ministers for **guidance** on the following elements:

- Do you think that the current approach as proposed by the presidency on the permitted **processing of metadata** is an acceptable basis to move forward? What other improvements could be made?
- Do you consider the approach concerning the **protection of terminal equipment and privacy settings** to be an acceptable basis to move forward?
- Do you think that the latest compromise proposed by the presidency enhances the **competitiveness of the European industry** in providing innovative services while, at the same time, safeguarding the **confidentiality of citizens' communications and the protection of citizens' data** (or sensitive data)?

How will the text become law? For it to be adopted, the text will need to be approved by both the Council and the European Parliament. The Parliament adopted its negotiating mandate in October 2017.

Digital single market for Europe

Cybersecurity agency and cybersecurity certification

The Council is due to agree its position, called a '**general approach',** on a proposal to upgrade the current European Union Agency for Network and Information Security (ENISA) into a **permanent EU agency for cybersecurity** and to create an **EU-wide certification framework for information and communication technology (ICT) products and services** (Commission proposal; draft Council general approach).

The proposal, known as the **Cybersecurity Act**, is part of the 'Cybersecurity package' presented by the Commission in September 2017. It aims to establish a high level of cybersecurity and cyber resilience within the EU, as well as to increase trust in ICT-based products and improve the functioning of the single market.

EU agency for cybersecurity

The EU Agency for Network and Information Security (ENISA) was set up in 2004 in Greece, and its current mandate runs until 2020. The agency acts as a centre of information and knowledge to enhance network and information security in the EU and support capacity building in member states.

Cybersecurity challenges faced by the EU have evolved and increased significantly since the ENISA mandate was last updated in 2013. In addition, the adoption of the first EU legal act on cybersecurity in 2016 - the network and information security (NIS) directive - gave ENISA a key role in supporting the implementation of the directive.

The proposal will grant ENISA a permanent mandate and clarify its role as the EU agency for cybersecurity. It will give ENISA new tasks in supporting member states, EU institutions and other stakeholders on cyber issues. The tasks would include for example organising EU-level cybersecurity exercises and supporting and promoting EU policy on cybersecurity certification.

EU-wide cybersecurity certification

The purpose of cybersecurity certification is to provide grounds for confidence to users about the security of ICT processes, products and services. Information on cybersecurity features is becoming increasingly important as increased digitisation and connectivity have led to increased cybersecurity risks. And this trend is set to continue, with the expected rapid expansion of connected objects ('Internet of Things') ranging from connected cars to health tracking devices and smart home appliances.

Currently, a number of different security certification schemes exist in the EU. As a consequence, a company may need to undergo several, often costly, certification procedures in various EU countries to be able to offer its product on multiple markets.

In order to tackle market fragmentation and make information more transparent, the proposed regulation sets out to create a framework and mechanism for setting up specific certification schemes for ICT processes, products and services ('European cybersecurity certification schemes'). Under these schemes, an independent third-party body would evaluate a product or service against a defined set of criteria, and issue a certificate. These will be valid in all EU countries, making it easier for consumers to understand the security features of a product or service, and for companies to carry out their business across borders.

Features covered would include for instance the ability to protect data against unauthorised storage or accidental loss or alteration.

Certification would be voluntary unless otherwise specified in EU law or member states' law. The schemes would make full use of existing standards, such as those developed by the European standardisation organisations.

The presidency **compromise proposal** introduces a number of changes to the proposal. For example, it adds ICT processes to the scope of certification schemes. It defines the role of the member states and industry in the initiation and preparation of certification schemes. It also introduces the possibility for a conformity self-assessment by the manufacturer or provider of ICT products and services, although only for low-risk products or services. New provisions have been added on the right to lodge a complaint and the right to an effective judicial remedy in the context of certification. In addition, a national liaison officers network would be set up to facilitate information sharing between ENISA and the member states.

The **European Council** has highlighted the importance of EU cybersecurity measures on several occasions. In October 2017 it stated that the Commission's cybersecurity proposals should be "delivered timely and examined without delay, on the basis of an action plan to be set up by the Council". In March this year, it invited the EU and its member states to "continue to bolster their capabilities to address hybrid threats".

How will the text become law? Both the Council and the Parliament have to agree on the text before it can enter into force. The Parliament has not yet adopted its position.

Council conclusions on building strong cybersecurity for the EU

Action plan for the implementation of cybersecurity conclusions

Joint communication Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

Reform of cyber security in Europe

Digital single market for Europe

ENISA website

Re-use of public sector information

The Council will hold a **policy debate** on a draft directive to **promote the re-use of public sector information** (PSI). The proposal aims to strengthen the EU's data economy by increasing the amount of public sector data available for re-use, ensuring fair competition and encouraging cross-border innovation based on data.

The public sector in the EU produces vast amounts of data such as meteorological data, digital maps and statistics. This information is a valuable source for society and the economy. Therefore, the EU has for many years been encouraging member states to make as much information available for re-use as possible.

Under the current PSI directive, all content that is available under national laws on access to documents is, in principle, re-usable beyond its initial purpose of collection, including for commercial purposes. This applies to public bodies at national, regional and local levels, such as ministries, state agencies and municipalities, as well as organisations funded mainly by or under the control of public authorities. Content held by museums, libraries and archives is also covered, but some special rules apply.

Charges for re-use should, in principle, be limited to the marginal costs of the request, including reproduction, provision and dissemination costs, and public bodies are encouraged to apply lower charges or no charges at all.

The Commission has now reviewed the current directive and is proposing updated rules to take account of technological changes and to tackle a number of shortcomings which prevent small and medium-sized enterprises from fully exploiting the potential of public sector information.

The proposed new rules include the requirement for public sector bodies to make dynamic data (e.g. 'real-time' data coming from sensors or satellites) immediately available through an 'application programming interface' (API) for maximum impact. The proposal also introduces a specific category of 'high-value datasets' whose re-use is associated with important socio-economic benefits. In principle, the re-use of such high-value datasets should be free of charge.

The updated directive would also cover data from research financed from public funds, which should be made available at no charge.

The Commission presented its proposal in April, together with several other data-related initiatives that seek to create a common European data space to boost the development of new products and services based on data.

The **Council's policy debate** will be structured around a set of questions prepared by the presidency in a background document. The questions are as follows:

- Do you agree that Europe's competitiveness requires the availability of public data as a key resource for innovation, new products and artificial intelligence applications?
- Given the potential of public sector information as a source of innovation and the speed of technological change, do you agree that European open data policy should include, in particular as regards the bodies and areas to be covered, the possibility to re-use dynamic data and the availability of high-value datasets for re-use?

Ministers' views will provide guidance for future work on the proposal in the Council working party.

How will the text become law? For it to be adopted, the text must be approved by both the Council and the European Parliament. The Parliament has not yet adopted its position.

Digital single market for Europe

Other business

- Directive on the European Electronic Communications Code
- Regulation on the Body of European Regulators for Electronic Communications (BEREC)
  Information from the presidency

  Electronic Communications Code
- Regulation on a framework for the free flow of non-personal data in the European Union
  Information from the presidency
- Digital single market
  Information from the Commission on the state of play
- Work programme of the incoming presidency
  Information from the Austrian delegation